ABSTRACT OF THE DISCLOSURE

When a flash unlock routine unlocks the flash memory to permit updating of a BIOS image, a message is left in secure non-volatile memory, such as a EEPROM. Upon the next re-boot, the boot block code will detect the special message in the non-volatile memory and perform a signature verification of the next block of code that is to be executed during the POST process. This code block will check the remainder of the BIOS image before POST proceeds.

09945328.082401